In 3

AUTHORITIES CITED IN CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT (Standard Form 189)

NEWARK PUBLIC LIBRARY

JUN 1 1 1986

U. S. GOVT. PUBS.
DEPOSITORY 326

April 1986

U.S. Department of Transportation
Office of the Secretary of Transportation
Office of Security

TD 1.2:

The purpose of this pamphlet is to provide a copy of the authorities cited in the Classified Information Nondisclosure Agreement (Standard Form 189). The pamphlet also contains some questions and answers that may be helpful when signing this form.

If you have any questions or doubts pertaining to the SF 189, please consult your Security Office. The DOT/OST Security Office may be contacted at FTS 426-4677 or Commercial (202) 426-4677.

Title 18, United States Code

§ 641. Public money, property or records

Whoever embezzles, steals, purloins or knowingly coverts to his use or the use of another, or without authority, sells, conveys or disposes of any records, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being under contract for the United States or any department or agency thereof or;

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1,000 or imprisoned not more than one year or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

§ 793. Gathering, transmitting or losing defense information

(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, research laboratory or station or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or

other materials or instruments for use in time of war are being made, prepared, repaired, stored, or are the subject of research or development, under any contract or agreement with the Untied States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document writing, or note of anything connected with the national defense; or

(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made or disposed of by any person contrary to the provisions of this chapter; or

(d) Whoever lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be com-

municated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

(e) Whoever having unauthorized possession of, access to, or control over any documents, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more

of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

Title 18, United States Code

§ 794. Gathering or delivering defense information to aid foreign governmet

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly any document, writing code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(b) Whoever, in time of war, with intent that the same shall be communicated to the enemy, collects, records, publishes, or communicates, or attempts to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the Armed Forces, ships, aircraft, or war materials of the United States or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties

READEX FICHE best copy available

to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

Title 18, United States Code

§ 798. Disclosure of classified information

(a) Whoever knowingly and willfully communicates, furnishes, transmits, or otherwise makes available to an unauthorized person, or publishes, or uses in any manner prejudicial to the safety or interest of the United States or for the benefit of any foreign government to the detriment of the United States any classified information—

(1) concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or

(2) concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or

(3) concerning the communication intelligence activities of the United States or any foreign government; or

(4) obtained by the process of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

(b) As used in subsection (a) of this section—

The term "classified information" means information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution;

The terms "code," "cipher," and "cryptographic system" include in the their meanings, in addition to

their usual meanings, any method of secret writing and any mechnical or electrical device or method used for the purpose of disguising or concealing the contents, significance, or meanings of communications;

The term "foreign government" includes in its meaning any person or persons acting or purporting to act for or on behalf of any faction, party, department, agency, bureau, or military force of or within a foreign country, or for or on behalf of any government or any person or persons purporting to act as a government within a foreign country, whether or not such government is recognized by the United States;

The term "communication intelligence" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

The term "unauthorized person" means any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States.

(c) Nothing in this section shall prohibit the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States of America, or joint committee thereof.

Title 18, United States Code

§ 592. Diplomatic codes and correspondence

Whoever, by virture of his employment by the United States, obtains from another or has or has had custody of or access to, any official diplomatic code, or which purports to have been prepared in any such code, and without authorization or competent authority, willfully publishes or furnishes to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both.

Title 50, United States Code

§ 783. Offenses

(b) Communication of classified information by Government officer or employee

It shall be unlawful for any officer or employee of the United States or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the United States or any department or agency thereof, to communicate in any manner or by any means, to any other person whom such officer or employee knows or has reason to believe to be an agent or representative of any foreign government or an officer or member of any Communist organization as defined in paragraph (5) of section 782 of this title, any information of a kind which shall have been classified by the President (or by the head of any such department, agency, or corporation with the approval of the President) as affecting the security of the United States, knowing or having reason to know that such information has been so classified, unless such officer or employee shall have been specifically authorized by the President, or by the head of the department, agency, or corporation by which this officer or employee is employed, to make such disclosure of such information.

TITLE VI—PROTECTION OF CERTAIN NATIONAL SECURITY INFORMATION [1]

PROTECTION OF IDENTITIES OF CERTAIN UNITED STATES UNDERCOVER INTELLIGENCE OFFICERS, AGENTS, INFORMANTS, AND SOURCES

SEC. 601.(a) Whoever, having or having had authorized access to classified information that identifies a covert agent, intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more that $50,000 or imprisoned not more than ten years, or both.

(b) Whoever, as a result of having authorized access to classified information, learns the identity of a covert agent and intentionally discloses any information identifying such covert agent to any individual not authorized to receive classified information knowing that the information disclosed so identifies such covert agent and that the United States is taking affirmative measures to conceal such covert agent's intelligence relationship to the United States, shall be fined not more than $25,000 or imprisoned not more than five years, or both.

(c) Whoever, in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, discloses any information that identifies as a covert agent to any individual not authorized to receive classified information, knowing that the information disclosed so identifies such individual and that the United States is taking affirmative measures to conceal

[1] Title VI was added by the *Intelligence Identities Protection Act of 1982* (Public Law 97-200).

such individual's classified intelligence relationship to the United States, shall be fined not more than $15,000 or imprisoned not more than three years, or both.

DEFENSES AND EXCEPTIONS

SEC. 602.(a) It is a defense to a prosecution under section 601 that before the commission of the offense with which the defendant is charged, the United States had publicly acknowledged or revealed the intelligence relationship to the United States of the individual the disclosure of whose intelligence relationship to the United States is the basis for the prosecution.

(b)(1) Subject to paragraph (2), no person other than a person committing an offense under section 601 shall be subject to prosecution under such section by virture of section 2 or 4 of title 18, United States Code, or shall be subject to prosecution for conspiracy to commit an offense under such section.

(2) Paragraph (1) shall not apply (A) in the case of a person who acted in the course of a pattern of activities intended to identify and expose covert agents and with reason to believe that such activities would impair or impede the foreign intelligence activities of the United States, or (B) in the case of a person who has authorized access to classified information.

(c) It shall not be an offense under section 601 to transmit information described in such section directly to the Select Committee on Intelligence of the Senate or to the Permanent Select Committee on Intelligence of the House of Representatives.

(d) It shall not be an offense under section 601 for an individual to disclose information that solely identifies himself as a covert agent.

REPORT

SEC. 603. (a) The President, after receiving information from the Director of Central Intelligence, shall submit to the Select Committe on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives an annual report on

measures to protect the identities of covert agents, and on any matter relevant to the protection of the identities of covert agents.

(b) The report described in subsection (a) shall be exempt from any requirement for publication or disclosure. The first such report shall be submitted no later than February 1, 1983.

EXTRATERRITORIAL JURISDICTION

SEC. 604. There is jurisdiction over an offense under section 601 committed outside the United States if the individual committing the offense is citizen of the United States or an alien lawfully admitted to the United States for permanent residence (as defined in section 101(s)(20) of the Immigration and Nationality Act).

PROVIDING INFORMATION TO CONGRESS

SEC. 605. Nothing in this title may be construed as authority to withhold information from the Congress or from a committee of either House of Congress.

DEFINITIONS

SEC. 606. For the purpose of this title:

(1) The term "classified information" means information or material designated and clearly marked or clearly represented, pursuant to the provisions of a statute or Executive order (or a regulation or order issued pursuant to a statute or Executive order), as requiring a specific degree of protection against unauthorized disclosure for reasons of national security.

(2) The term "authorized", when used with respect to access to classified information, means having authority, right or permission pursuant to the provisions of a statute, Executive order, directive of the head of any department or agency engaged in foreign intelligence or counterintelligence activities, order of any United States court, or provisions of any Rule of the House of Representatives or resolution of the Senate which assigns responsibility within the respective

House of Congress for the oversight of intelligence activities.

(3) The term "disclose" means to communicate, provide, impart, transmit, transfer, convey, publish, or otherwise make available.

(4) The term "covert agent" means—

(A) an officer or employee of an intelligence agency or a member of the Armed Forces assigned to duty with an intelligence agency—

(i) whose identity as such an officer, employee, or member is classified information, and

(ii) who is serving outside the United States or has within the last five years served outside the United States; or

(B) a United States citizen whose intelligence relatlionship to the United States is classified information, and—

(i) who resides and acts outside the United States as an agent of, or informant or source of operational assistance to, an intelligence agency, or

(ii) who is at the time of the disclosure acting as an agent of, or informant to, the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation; or

(C) an individual, other than a United States citizen, whose past or present intelligence relationship to the United States is classified information and who is a present or former agent of, or a present or former informant or source of operational assistance to, an intelligence agency.

(5) The term "intelligence agency" means the Central Intelligence Agency, a foreign intelligence component of the Department of Defense, or the foreign counterintelligence or foreign counterterrorism components of the Federal Bureau of Investigation.

(6) The term "informant" means any individual who furnishes information to an intelligence agency in the course of a confidential relationship protecting the identity of such individual from public disclosure.

(7) The terms "officer" and "employee" have the meanings given such terms by section 2104 and 2105, respectively, of title 5, United States Code.

(8) The term "Armed Forces" means the Army, Navy, Air Force, Marine Corps, and Coast Guard.

(9) The term "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(10) The term "pattern of activities" requires a series of acts with a common purpose or objective.

Questions and Answers for Use With the Classifed Information Nondisclosure Agreement (SF-189)

QUESTION 1. What is its purpose since a security clearance has already been granted, and there are Federal laws which safeguard national security information already?

Answer: The granting of a security clearance is a conditional determination of trustworthiness by a U.S. agency of an employee who will require access to classified information to accomplish official duties. By itself, the clearance establishes no expressed obligations on the part of the employee or the Government. On the other hand, the SF-189 serves as a contractual agreement between the U.S. Government and the cleared employee in which the employee agrees never to disclose classified information to an unauthorized person.

Usually the form is signed by the employee at the time security clearance is granted. The agreement specifies the rights and duties of the parties. In addition, the contractual relationship, as interpreted by the Supreme Court, provides the Government with a clear basis to prevent or punish unauthorized disclosures. The granting of a clearance provides no specified contractual remedy for the Government except the clearance's possible withdrawal.

QUESTION 2. What is the authority for the SF-189?

Answer: The legal basis for implementation of the SF-189 is National Security Decision Directive (NSDD) 84. NSDD-84 directed the developemnt of two nondisclosure agreement forms for Government-wide use. One of these forms, the Classified Information Nondisclosure Agreement, SF-189, was promulgated by the Information Security Oversight Office as required by Section 1a of the Directive.

QUESTION 3. What effect does the SF-189 have on the DOT Form 1600.9, Security Acknowledgement Statement?

Answer: The SF-189 replaces the DOT Form 1600.9.

QUESTION 4. Does the SF-189 which an employee of an agency signs only apply to that time during which he or she is employed by the agency?

Answer: When an employee signs the SF-189, he/she enters into a contractural agreement that is binding

during the time the employee is granted access to classified information, and at all times thereafter. Clearly, the injury to the United States that may result from unauthorized disclosures of classified information does not end with a person's employment. The agreement is designed so that an employee will only need to sign one nondisclosure agreement regardless if she/he changes employers. The SF-189 shall be retained by the Department for 50 years. DOT requires all new employees to sign a SF-189.

QUESTION 5. Paragraph number 1 includes a statement that the nondisclosure agreement encompasses material which is "classifiable" and therefore would indicate that any material a person may be dealing with which is not necessarily classified, but becomes classified in the future cannot be released. What does the term "classifiable" mean, and how can a person who after his/her Federal Government employment be held responsible for releasing classified information which was not classified when he/she had access to it while employed in the Federal Government?

Answer: The term "classifiable" refers to information that meets the criteria for classification under Executive Order 12356, National Security Information, but which has not yet been properly marked because of time limitations, oversight or error. For example, if an employee is briefed on a project that involves classified infor-

mation, the notes taken, before they are reviewed and appropriately stamped to indicate their classification, are "classifiable." An employee with authorized access to classified information would only be liable for disclosing "classifiable" information when he/she reasonably should have known that the information met the tests for classification and should have been marked as such.

QUESTION 6. Do paragraph numbers 3, 5 and 6 infringe upon the First Amendment guarantees of freedom of speech and of the press, particularly if they require prepublication approval or censorship of future written work?

Answer: The SF-189 does not require prepublication review. As interpreted by the Supreme Court, the provisions of paragraphs 3, 5 and 6, as well as the rest of the SF-189, do not infringe on First Amendment rights.

QUESTION 7. To what extent would paragraph number 3 require a signer of the SF-189 to presubmit any written materials he/she might contemplate publishing in the future to a Federal Government Agency for clearance? To what agency would he/she submit them?

Answer: Since the SF-189 does not contain a prepublication provision, the signer of the form is not required to submit any written materials before they are published.

However, if an individual who is or has been employed by the Government is concerned that something he/she has prepared for publication may contain

classified information, that individual should be encouraged to submit it to his/her current or last employing agency for a voluntary review.

QUESTION 8. Regarding paragraph 5 of SF-189:

a. What is the statutory authority for this provision?

b. Can a signer of the SF-189 be held liable under this provision for releasing information from publically available sources which become classified after these sources were published, but the sources were never sanitized or destroyed.

Answer: a. In Snepp v. United States, 444 U.S. 507 (1980), the Supreme Court held that Snepp, a former CIA empoloyee, breached his fiduciary obligation arising from an employment agreement when he failed to submit his manuscript for prepublication review. The proceeds of his breach were impressed with a constructive trust for the benefit of the Government.

b. Liabililty would depend on the circumstances of the case. In the case cited, it is unclear whether the signer had any knowledge that the information from publicly available sources became classified after the sources were published. Therefore, the Information Security Oversight Office cannot make a blanket ruling on such limited information.

QUESTION 9. What are the remedies available to the Federal Government to enforce the provisions of SF-189 other than the one cited in Paragraph number 6?

Answer: In addition to the Government's right to seek a court injunction prohibiting disclosure of classified information, mentioned in paragraph 6 of the SF-189, the sanctions mentioned in paragraph 5 also apply. Furthermore, depending upon the circumstances of the case, the Government has the right to take a variety of administrative or legal steps including:

a. imposition of penalties prescribed for security violations;

b. revocation of an individual's security clearance;

c. imposition of appropriate administrative sanctions up to and including transfer of an individual away from a sensitive position or termination of Government employment;

d. assessment of any financial penalties that may be provided by contract between the Government and the contractor; and

e. initiation of criminal prosecution against an individual, if approved by the Department of Justice.

QUESTION 10. Does the provision of Paragraph number 7 intend to mean that the information which was classified when the signer of the SF-189 had access to it cannot be revealed by that per-

son even after it is declassified and it has entered the public domain?

Answer: The restrictions on persons executing the SF-189 do not apply to information that has been officially declassified. However, there may be requirements imposed by other authorities that require continued withholding from public disclosure despite the information's declassification. Therefore, we cannot provide a blanket interpretation that declassification always equals authorization for disclosure.

QUESTION 11. Do I need to show the SF-189 to an attorney before I sign it?

Answer: It is entirely up to you whether you show the SF-189 to a lawyer. We believe the Agreement is simple and straightforward. If we agree to provide you with access to classified information, you agree never to disclose the information to an unauthorized party.

QUESTION 12. Will the Government pay for the cost of an attorney?

Answer: No. In this and similar situations, you must pay for your own lawyer.

QUESTION 13. What will the government do if I refuse to sign the SF-189?

Answer: The Government will not provide you with access to classified information or, if you now have such access, it will initiate action to revoke your security clearance, terminating your access. If your current access is terminated, you will still have to abide

by the terms of any agreement that you previously signed.

QUESTION 14. Can I keep a signed copy of the SF-189?

Answer: The SF-189 itself is not classified, but it is the policy of DOT that the individual not be given a signed copy of the SF-189. He/she may have a copy of a blank SF-189.

QUESTION 15. Paragraph 2 indicates that I have received a security indoctrination. What happens if, after receiving this indoctrination, I decide not to sign the SF-189?

Answer: The indoctrination is not classified, and you will be given access to classified information only after you sign the nondisclosure agreement.

QUESTION 16. In paragraph 3, what is meant by "indirect unauthorized disclosure"?

Answer: One example of indirect unauthorized disclosure would be if, instead of relating classified details about a project, you told an unauthorized individual where he might obtain the information, for instance, that he should read the story on pages 30-33 of a particular magazine because it was entirely accurate.

QUESTION 17. Certain information that I know to be classified has appeared in a newspaper article. Can I consider this information declassified and freely quote the article and disseminate the

information without obtaining prior written authorization?

Answer: An unauthorized disclosure of classified information does not result in declassification of the information. Of course, in the abstract, merely quoting a newspaper article is not a problem.

QUESTION 18. In paragraph 4, what is the meaning of the sentence, "Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for my statutory violation?"

Answer: It means that you may be prosecuted for any law you may have violated, not just the laws specifically mentioned in this Agreement.

QUESTION 19. Paragraph 8 uses the term "authorized representative." What is meant by this term?

Answer: By authorized representative, it is meant the agency head or his designee. Ordinarily, responses to questions relating to this Agreement will come from the local security manager within your department/agency.

QUESTION 20. Does paragraph 8 mean that my obligations under this Agreement apply even if I do not currently have access to classified information and even if I am no longer employed by the Government?

Answer: Yes. You are obligated to protect classified information from unauthorized disclosure in perpetuity from the time you receive access to this material.

QUESTION 21. Can any of the language in the SF-189 be altered to suit the preferences of an individual signer?

Answer: The SF-189 has been approved by the National Security Council, and the Department of Justice has rendered the decision that the form as written is enforceable in a court of law. Therefore, its language may not be unilaterally altered.

#00074—5/86

☆ U. S. GOVERNMENT PRINTING OFFICE : 1986 491-810/20749